WHAT IS CLAIMED IS:

1. A copy management system, comprising:

a storage media, which is stored with content encrypted with an encryption key, is attached with unique media identification information, and is distributed from an administrator side to a user;

a terminal device for user, which comprises copy means for decrypting the content stored in the storage media by a decryption key corresponds to the encryption key and coping decrypted content to secondary storage media, and which transmits predetermined and unique device identification information together with the media identification information when copying the content;

a management server device, which transmits the decryption key against the terminal device corresponds to the device identification information when receiving the media identification information.

2. The copy management system according to claim 1, wherein the management server device transmits the decryption key only once against one media identification information.

3. The copy management system according to claim 2, wherein the terminal device transmits, as the device identification information, at least one of identification information attached uniquely to the terminal device, the

identification information attached uniquely to the copy means, and the identification information uniquely attached to memory connected to the terminal device.

4. The copy management system according to claim 1, wherein

the management server device encrypts the decryption key by the device identification information, and

the terminal device decrypts the encrypted decryption key with own device identification information and uses it for decrypting the content.

5. The copy management system according to claim 1, wherein

the terminal device deletes the decryption key after decrypting the content.

6. The copy management system according to claim 1, wherein

the management server device transmits a re-encryption key for re-encrypting the content to be copied;

the terminal device re-encrypts the content decrypted with the decryption key using the re-encryption key and copies it;

the terminal device stores the re-encryption key in a storage means; and

the terminal device decrypts the copied content with the re-encryption key stored in the storage means and reproducing it when reproducing the copied content.

7. The copy management system according to claim 1, wherein

the management server device manages transmission of the decryption key by storing in a database, in a state of being associated with device identification information of each user's terminal device, the media identification information which the decryption key has been already transmitted; and

the management server device overwrites old device identification information registered in the database with new device identification information when the new device identification information is applied to the terminal device due to repair or exchange.

8. The copy management system according to claim 1, wherein

the management server device performs predetermined charge processing against a user who owns terminal device to which transmission of the decryption key is performed.

9. The copy management system according to claim 1, further comprising:

intermediating server device, which intermediates in the transmission/reception of information between the terminal device and the management server device, and which performs charge processing for the user at least when the decryption key is transmitted to the terminal device.

10. A computer readable storage media, which has been stored with a client terminal device information processing program,

the information processing program, comprising:

a step of reading out media identification information from a storage media attached with unique media identification information and which is stored with content encrypted with an encryption key;

a step of reading out device identification information uniquely attached to a device used when a user performs copying of the content;

a step of transmitting to an administrator side server device at least the read out media identification information and device identification information;

a step of receiving a decryption key returned from the administrator side server device through transmission of the media identification information and device identification information;

a step of performing decryption processing of content stored in the storage media using the received decryption key; and

a step of copying decrypted content.

11. The computer readable storage media, which has been stored with client terminal device information processing program, according to claim 10, wherein

the step of receiving a decryption key comprises a step

of receiving a decryption key, which is encrypted with device identification information of a user device and transmitted; and

the step of performing decryption processing of content comprises: a step of performing decryption processing of the encrypted decryption key with device identification information of own device; and a step of performing decryption processing of content stored in the storage media using the decryption processed decryption key.

12. The computer readable storage media, which has been stored with client terminal device information processing program, according to claim 10, further comprising:

a step of deleting the decryption key after copying the content.

13. The computer readable storage media, which has been stored with client terminal device information processing program, according to claim 10, further comprising:

a step of receiving a re-encryption key for re-encrypting the content to be copied, which is transmitted from the management server device;

a step of re-encrypting with the re-encryption key the content decrypted with the decryption key and copying it;

a step of storing the re-encryption key in a storage means; and

a step of decrypting the copied content with the re-encryption key stored in the storage means and reproducing it when reproducing the copied content.

14. The computer readable storage media, which has been stored with client terminal device information processing program, according to claim 10, wherein

the step of transmitting the media identification information and device identification information comprises a step of transmitting, as the device identification information, at least one of identification information attached uniquely to the terminal device which user uses, the identification information attached uniquely to secondary storage media which the content is to be copied, and the identification number attached uniquely to memory connected to the terminal device.

15. A computer readable storage media, which has been stored with a management server device information processing program,

the information processing program comprising:

a step of receiving device identification information, which are sent from a user device and which is uniquely attached to the user device, and media identification information uniquely attached to a storage media stored with content encrypted with an encryption key;

a step of detecting whether the received media identification information is registered in a database registered with media identification information of storage media having the content thereof copied in a state of being associated with device identification information of each user device; and

a step of transmitting a decryption key for decrypting the content to a user device when non-registration of the media identification information is detected.

16. The computer readable storage media, which has been stored with a management server device information processing program, according to claim 15, further comprising:

a step of registering in the database the media identification information which the decryption key is transmitted in a state of being associated with device identification information of a user device which the decryption key is transmitted.

17. The computer readable storage media, which has been stored with a management server device information processing program, according to claim 16, wherein

the step of transmitting a decryption key comprises a step of encrypting the decryption key with device identification information of the user device and transmits the encrypted decryption key.

18. The computer readable storage media, which has been stored with a management server device information processing program, according to claim 17, wherein

the step of transmitting a decryption key comprises a step of transmitting a re-encryption key for re-encrypting the content to be copied.

19. The computer readable storage media, which has been stored with a management server device information processing program, according to claim 15, further comprising:

a step of overwriting old device identification information registered in the database with new device identification information when new device identification information is applied to the user device due to repair or exchange.

20. The computer readable storage media, which has been stored with a management server device information processing program, according to claim 15, further comprising:

a step of charging a user who has performed transmission of the decryption key.

21. The computer readable storage media, which has been stored with a management server device information processing program, according to claim 15, wherein

the step of receiving the media identification

information and device identification information comprises a step of receiving, as the device identification information, at least one of identification information attached uniquely to the terminal device which user uses, the identification information attached uniquely to secondary storage media which the content is to be copied, and the identification number attached uniquely to memory connected to the terminal device.

22. A copy management method comprising the steps of:

transmitting to a management server device, device identification information and media identification information from a device when copying content encrypted with an encryption key and stored in a storage media having uniquely attached media identification information by a user device having uniquely attached device identification information;

detecting by the management server device whether or not the media identification information that is transmitted from the user device is registered in a database registered with media identification information of storage media having the content thereof copied in a state of being associated with device identification information of each user device; and

transmitting a decryption key for decrypting the content to the user device when non-registration of the media identification information is detected.

23. A client terminal device information processing method, comprising the steps of:

reading out media identification information from a storage media attached with unique media identification information and which is stored with content encrypted with an encryption key;

reading out device identification information uniquely attached to a device used when a user performs copying of the content;

transmitting to an administrator side server device at least the read out media identification information and device identification information;

receiving a decryption key returned from the administrator side server device through transmission of the media identification information and device identification information;

performing decryption processing of content stored in the storage media using the received decryption key; and

copying the decrypted content.

24. A management server device information processing method, comprising the steps of:

receiving device identification information, which are sent from a user device and which is uniquely attached to the user device, and media identification information uniquely attached to a storage media stored with content encrypted with

an encryption key;

detecting whether or not the received media identification information is registered in a database registered with media identification information of storage media having the content thereof copied in a state of being associated with device identification information of each user device; and

transmitting a decryption key for decrypting the content to a user device when non-registration of the media identification information is detected.

25. A client terminal device information processing program, comprising:

a step of reading out media identification information from a storage media attached with unique media identification information and which is stored with content encrypted with an encryption key;

a step of reading out device identification information uniquely attached to a device used when a user performs copying of the content;

a step of transmitting to an administrator side server device at least the read out media identification information and device identification information;

a step of receiving a decryption key returned from the administrator side server device through transmission of the media identification information and device identification

information;

a step of performing decryption processing of content stored in the storage media using the received decryption key; and

a step of copying the decryption processed content.

26. A management server device information processing program, comprising:

a step of receiving device identification information, which are sent from a user device and which is uniquely attached to the user device, and media identification information uniquely attached to a storage media stored with content encrypted with an encryption key;

a step of detecting whether or not the received media identification information is registered in a database registered with media identification information of storage media having the content thereof copied in a state of being associated with device identification information of each user device; and

a step of transmitting a decryption key for decrypting the content to a user device when non-registration of the media identification information is detected.